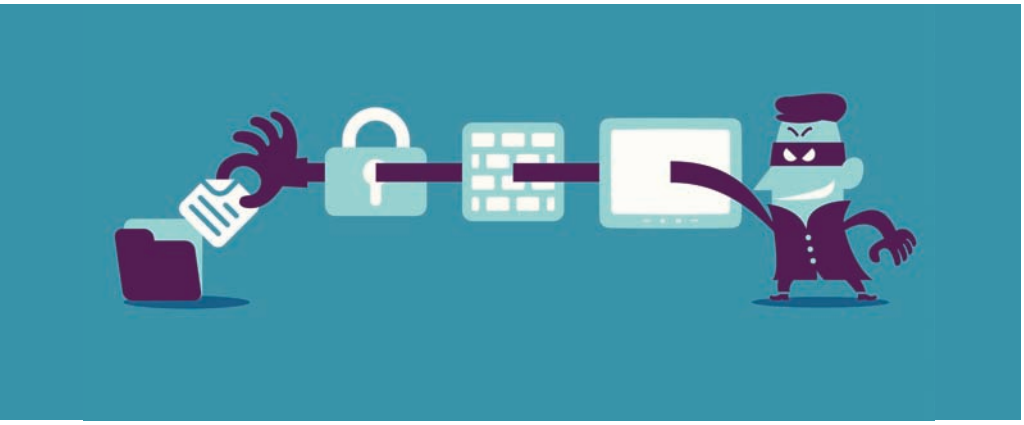
Risk Management



RANSOMWARE: Minimizing the Risks

By Justin Pope, JD

Innov Clin Neurosci. 2016;13(11–12)37–40

This ongoing column is dedicated to providing information to our readers on managing legal risks associated with medical practice. We invite questions from our readers. The answers are provided by PRMS, Inc. (www.prms.com), a manager of medical professional liability insurance programs with services that include risk management consultation, education and onsite risk management audits, and other resources to healthcare providers to help improve patient outcomes and reduce professional liability risk. The answers published in this column represent those of only one risk management consulting company. Other risk management consulting companies or insurance carriers may provide different advice, and readers should take this into consideration. The information in this column does not constitute legal advice. For legal advice, contact your personal attorney. Note: The information and recommendations in this article are applicable to physicians and other healthcare professionals so "clinician" is used to indicate all treatment team members.

QUESTION

I work in a small private practice with very limited IT support. Given recent national news headlines in which cyber attackers have targeted large healthcare systems and held patient information for ransom, should I be concerned as a solo practitioner?

ANSWER

Yes, healthcare providers of all sizes should be concerned about ransomware and other cyber attacks.

What is Ransomware?

Ransomware is a type of malicious software that seeks to infiltrate computer systems or connected devices in order to encrypt a user's files. Once the files have been encrypted, making the information indecipherable and inaccessible, the user receives a pop-up notification demanding payment of a ransom (usually in untraceable digital currency such as Bitcoin) in exchange for the decryption key.[1]

The History and Evolution of Ransomware

Although ransomware attacks have received increased publicity in the past year, it is not an entirely new threat. The first ransomware virus was disseminated almost 30 years ago when Dr. Joseph Popp, a World Health Organization consultant and AIDS researcher, mailed 20,000 informational floppy disks containing ransomware to a group of international conference attendees. The virus encrypted computer files and demanded that the victims send $189 dollars to a physical mailing address. Dr. Popp's ransomware virus, popularly known as the "AIDS Program," was the first cyber attack of its kind.[2]

Cyber criminals now deliver ransomware in a variety of ways. Hackers most frequently use spam emails, or unwanted commercial emails, containing ransomware to bypass a user's technical safeguards and initiate encryption. Ransomware attacks may also take place by way of phishing campaigns in which hackers send emails purported to be from a legitimate source requesting passwords or other sensitive information. Many IT experts increasingly fear the use of online advertising to transmit ransomware—a tactic known as "malvertising."[3]

Ransomware in the News

A few of the most notable healthcare ransomware attacks of 2016 include the following:

- Hollywood Presbyterian Medical Center (HPMC), in Los Angeles, California, made national news headlines last February when it was widely reported they paid hackers $3.4 million in Bitcoin for a decryption key after being locked out of their computer systems. HPMC later released a

statement denying those reports, but confirming they did pay a $17,000 ransom in the interest of quickly restoring hospital operations in order to provide patient care. Many people have been critical of HPMC's decision to pay the ransom and argue that this decision may have been directly responsible for a number of subsequent healthcare ransomware attacks.[4]

- Methodist Hospital (Henderson, Kentucky) announced an internal state of emergency last March after being infected by a ransomware variant known as "Locky." The attack limited Methodist's access to all web-based and electronic communications, and the hospital was forced to power down desktop computers in order to isolate the virus. Hackers demanded a $1,600 ransom but reportedly relented after Methodist restored its IT systems using backup data.[4]

- Also in March of 2016, Medstar Health (Baltimore, Maryland) became the target of a ransomware attack that prevented Medstar facilities from accessing patient data, making it necessary to postpone patient appointments and surgical procedures in some cases. Hackers threatened to destroy the decryption key and render records permanently inaccessible if Medstar did not pay $19,000 in Bitcoin within the next 10 days. Medstar was also given the option to decrypt a single computer for $1,250 in Bitcoin.[5]

- Kansas Heart Hospital in Witchita could no longer access patient files after its servers suffered a ransomware attack last May. When Kansas Heart paid the initial ransom requested by cyber attackers, hackers responded by decrypting only a portion of the stolen information. The hackers then made a new ransom demand for the rest of the encrypted patient information. Kansas Heart did not make a second ransom payment.[6]

Why Should You Be Concerned?

Standard of care. Ransomware attacks may make it difficult for you to provide quality patient care. A ransomware attack may affect your ability prevent you from accessing electronic health records (EHRs), patient emails, and electronic billing and scheduling systems, which are essential to daily practice and your ability to meet the standard of care.

Federal law. Physicians who maintain patient information could be subject to federal privacy laws. Under HIPAA's Security Rule, covered entities are required to implement security measures that may help prevent the introduction of ransomware. Covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) when faced with a breach must then comply with the breach notification rule as well as face the possibility of civil monetary penalties. The Federal Trade Commission (FTC) has also recently expressed a willingness to bring enforcement action against those businesses that fail to reasonably safeguard consumer information in accordance with their privacy and security practices.[3]

State law. State law may even govern the privacy and security of patient information. If a breach of patient information violates state law, an attorney general's office may be compelled to open an investigation. Parties affected by the breach could also have a private cause of action under state law.

What Steps Should You Take to Prevent Ransomware?

Resources from the United States Office for Civil Rights (OCR), Federal Bureau of Investigation (FBI), and Federal Trade Commission suggest the following prevention steps:

1. Understand ransomware attacks happen all the time. The United States Department of Justice now estimates that an average of 4,000 ransomware attacks occur daily. This figure represents a 300-percent increase in ransomware activity seen at this point last year.[1] Recent reports also indicate the healthcare industry may be targeted by ransomware attacks more frequently than any other industry. Cyber security provider Solutionary found the healthcare industry accounted for 88 percent of all ransomware detected last quarter.[7] Factors such as the value of healthcare records (partial records can sell for up to 50 times the value of credit card information on the black market, according to the FBI), the healthcare industry's transition to EHRs, and the lack of security technology utilized by smaller practices have contributed to an upsurge in healthcare ransomware attacks.[8]

2. Ensure all employees receive ransomware training. It is important that employees are made aware of the threat that ransomware poses and that they receive up-to-date training on the following:

- *Detecting malware*
  - ✓ Staff should be able to recognize when a link is

clicked, an attachment is opened, or a website is visited that might be malicious.
  - ✓ Staff should be able to recognize when the inability to access certain files is due to ransomware encryption, deletion, and/or renaming or relocating data.
- *Preventing ransomware*
  - ✓ Staff should be reminded to never open an email attachment unless they know what it is and trust the sender.
  - ✓ Staff should be reminded to never click on a link in an email message unless they know what it is and trust the sender.
  - ✓ Staff should be reminded to never install or download software on computers used by the practice—especially free software—without first confirming it is okay to do so.
  - ✓ Staff should understand what electronic information they are permitted to access and information is off limits.[9]

3. Backup important practice data and store offline. One of the most effective ways to protect your practice in the event of a ransomware attack is to back up sensitive and important information. Taking this step will allow you to restore your data and recover from a ransomware attack quickly. As some ransomware variants have been known to remove or otherwise encrypt online backups, practices should consider maintaining backups offline and unavailable from their networks.[9]

4. Encrypt sensitive practice data. Providers should consider encrypting and password protecting all patient information and devices. Per OCR's Ransomware and HIPAA Fact Sheet, a breach of protected health information that is actively encrypted and indecipherable at the time of a ransomware attack cannot be breached. Such a breach does not require a physician to give notice of the breach.[9]

5. Ensure basic technical safeguards have been implemented. Providers should ensure the implementation of the following technical safeguards:
- Up-to-date antivirus software on computers
- Enabled automated patches for operating systems and web browsers
- Complex passwords
- Pop-up blockers.[10]

6. Don't think it can't happen to your small practice. While ransomware attacks on large hospitals and health systems have been highly publicized, one must not forget that smaller private practices can also be at risk. In 2012, ABC reported that hackers encrypted emails and electronic health records maintained by Surgeons of Lake County, a small medical practice in Illinois. Hackers offered to make a decryption key available upon receipt of a ransom payment, but the medical practice responded by refusing to pay the ransom, shutting down their servers, and contacting the local authorities.[11]

As ransomware becomes more widely used by cyber criminals, private practitioners should expect to be targeted more often. The growing number of ransomware attacks is a direct result of the ease with which ransomware programs can now be acquired. Cyber gangs now host websites from which fairly simple ransomware programs can be downloaded by aspiring cyber attackers who, in return, pay a percentage of any ransom collected to the program creators.[3] Widespread availability of ransomware doesn't bode well for private practitioners with inadequate IT support and/or insufficient data security protocols in place, as this may make them attractive targets for cyber attacks.

7. Stay informed and current. Providers should stay up to date on the latest ransomware news and information. The United States government continues to provide resources to help providers protect against the threat of ransomware. Providers may also want to consider signing up for the OCR Security Listserv in order to receive ransomware updates and guidance.[12]

REFERENCES

1. The United States Department of Justice. How to protect your networks from ransomware. https://www.justice.gov/criminal-ccips/file/872771/download. Accessed October 10, 2016.
2. Taylor P. *Hackers: Crime in the Digital Sublime.* New York, NY: Routledge; 2005:109.
3. Ramirez E. Opening remarks. Presented at the FTC Fall Technology Series: Ransomware. Washington, D.C. 2016 Sept 7.
4. Mannion C. Three U.S. hospitals hit in string of ransomware attacks. NBC News. March 23, 2016. http://www.nbcnews.com/tech/security/three-u-s-hospitals-hit-string-ransomware-attacks-n544366. Accessed October 17, 2016.
5. Cox J. Medstar Health turns away patients after likely cyber attack. *The Washington Post*. March 29, 2016. https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-

f06b5ba21f33_story.html?utm_term=.5efa73b7a1f2. Accessed October 17, 2016.
6. Sun D. Hackers demand ransom payment from Kansas Heart Hospital for files. KWCH 12. May 20, 2016 http://www.kwch.com/content/news/Hackers-demand-ransom-payment-from-Kansas-Heart-Hospital-380342701.html. Accessed October 17, 2016.
7. NTT Security. Solutionary SERT Q2 report: eighty-eight percent of all ransomware is detected in healthcare industry. July 26, 2016. https://www.solutionary.com/threat-intelligence/threat-reports/quarterly-threat-reports/sert-threat-report-q2-2016/. Accessed October 12, 2016.
8. American Hospital Association. FBI Cyber Division. Health care systems and medical devices at risk for increased cyber intrusions for financial gain. April 8, 2014. http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf. Accessed October18, 2016.
9. U.S. Department of Health and Human Services. Fact sheet: ransomware and HIPAA. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed October 10, 2016.
10. Federal Bureau of Investigation. Incidents of ransomware on the rise: protect yourself and your organization. April 29, 2016. https://www.fbi.gov/news/stories/ransomware-on-the-rise. January 20, 2015. Accessed October 12, 2016.
11. Levin A. For ransom: your medical records. ABC New. August 22, 2012. http://abcnews.go.com/Business/ransom-medical-records/story?id=17051612. Accessed October 17, 2016.
12. U.S. Department of Health and Human Services. Sign up for the OCR Privacy & Security listserv. http://www.hhs.gov/hipaa/for-professionals/list-serve/. Accessed October 18, 2016.

AUTHOR AFFILIATION: Mr. Pope is Associate Risk Manager at PRMS, Inc. in Arlington, Virginia.

ADDRESS FOR CORRESPONDENCE:
Donna Vanderpool, MBA, JD,
Vice President, Professional Risk Management Services, Inc., 1401 Wilson Blvd., Suite 700, Arlington, VA 22209;
E-mail: vanderpool@prms.com